Notice of Allowability	Application No.	Applicant(s)	
	09/451,254	YACOBI ET AL.	
	Examiner	Art Unit	
	John M Winter	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the paper filed on May 22, 2003*.
2. ☒ The allowed claim(s) is/are *1-41 and 51-58*.
3. ☒ The drawings filed on *11/19/2002* are accepted by the Examiner.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.
5. ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
   (a) ☐ The translation of the foreign language provisional application has been received.
6. ☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application. **THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

7. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

8. ☐ CORRECTED DRAWINGS must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No. ____.
   (b) ☐ including changes required by the proposed drawing correction filed _____, which has been approved by the Examiner.
   (c) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No. _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet.

9. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1☒ Notice of References Cited (PTO-892)
2☐ Notice of Informal Patent Application (PTO-152)
3☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
4☐ Interview Summary (PTO-413), Paper No.____ .
5☐ Information Disclosure Statements (PTO-1449), Paper No. ____.
6☐ Examiner's Amendment/Comment
7☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
8☐ Examiner's Statement of Reasons for Allowance
9☐ Other .

Allowable Subject Matter

Claims 1-41 and 51-58 are allowed over the prior art record.

1. The following is an examiner's statement of reasons for allowance:

2. The closest prior art of record Briscoe (US Patent 6,341,273) teaches an electronic coin stick system comprising a chain of hash values generates using a secret number as a starting value. Schneier (Applied Cryptography, 2nd edition) teaches a protocol for exchanging encrypted mesages. Dykes et al (US Patent 5,872,915) teaches a user library wherein each protected software application has a table listing the user ID's of users entitled to access that software. Milner (WO 01/44968 A2) teaches a system for financial transactions based on notified changes of ownership of statically held tokens.
What they fail to teach or suggest:

A. minting a stick of electronic assets by digitally signing with an issuer's signature a composite of user provided data items including a user identity.

B. Spending on or more assets from the stick at on or more vendors, wherein each expenditure with a particular vendor involves digitally signing with a user's signature a first asset from the stick to be spent and passing the user-signed first asset along with the issuer-signed composite to the particular vendor for verification and subsequently passing any additional assets to be spent without user signature to the particular vendor.

These distinct features render claim 1 allowable.
Claims 2-11 are dependant upon claim 1 and have all of the limitations of claim 1, and are allowable for the same reasons

C. Signing the deposit request with a signature of the vendor: $S_V(S_U(C_J), CK, RL)$.
This distinct feature renders claim 6 allowable.

D. Forming a stick of electronic currency signed with the issuer's signature.
This distinct feature renders claim 12 and 51 allowable.
Claims 13-16, 18-23 are dependant upon claim 12 and have all of the limitations of claim 12, and are allowable for the same reasons
Claims 52-56 are dependant upon claim 51 and have all of the limitations of claim 51, and are allowable for the same reasons

E. Signing the withdrawal request with a signature of an issuer on the form of $S_I($ U,K,d,C_l, t,L) , wherein U is a user identity, K is a user secret, d is a denomination, C_l Is the value of the last asset taken from the bottom of the stick, t is an expiration time and L is a value.

This distinct feature renders claims 17 and 31 allowable.
Claims 32-33 are dependant upon claim 31 and have all of the limitations of claim 31, and are allowable for the same reasons

F. Creating at a user a stick of L electronic assets.
This distinct feature renders claim 24 allowable.
Claims 25-30 are dependant upon claim 24 and have all of the limitations of claim 24, and are allowable for the same reasons

G. Signing at he issuer, the withdrawal request by computing: $c= (p^{e}C_{l})^{Lf} = p^{L}C_{L}{}^{Lf}$.mod N
This distinct feature renders claim 34 allowable.
This distinct feature renders claim 34 allowable.
Claims 35-41 are dependant upon claim 34 and have all of the limitations of claim 34, and are allowable for the same reasons

H. Form a withdrawal request. Having a user identity U, a last asset value C_l taken from the bottom of the stick and the value L while omitting any vendor identity.
This distinct feature renders claim 57 allowable.

I. Signing the deposit request with a signature of the vendor: $S_V(C_J, Vi)$.
This distinct feature renders claim 58 allowable.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John M Winter whose telephone number is (703) 305-3971. The examiner can normally be reached on M-F 8:30-6, 1st Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James P Trammell can be reached on (703)305-9768. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 305-7687 for regular communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 308-1113.

JMW
May 29, 2003

JAMES P. TRAMMELL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600